Configuration Compliance Baseline Management in OpenManage Enterprise

Tech Note by:
Matthew Maze

SUMMARY

Configuration compliance baselines identify the difference between a chassis or server's settings and expected values. This feature is used to check and report attribute compliance throughout the data center.

This Direct from Development tech note summarizes the configuration compliance baseline feature and describes best-practice methods to get the most out of the feature.

Monitoring the attribute compliance of every device in your environment is difficult. Determining which device has, for example, a bad power setting or misconfigured user can be time consuming and frustrating. An important feature of OpenManage Enterprise (OME) is the ability to check the policy compliance of a device's attributes.

An attribute is a key value pair that describes a setting/state of a device. A device's attributes describe a range of functionality, from the type of iDRAC virtual console plugin to RAID virtual disk stripe size and many other functions. A device's attributes can change via a script, a power event or by modifying the values in the iDRAC or CMC. Sometimes modifying an attribute modifies other attributes in an unintended way. This can cause a device to behave in an undesired way. The configuration compliance feature in OpenManage Enterprise enforces datacenter policies by detecting and displaying the differences between a device's attributes and the desired attributes.

Achieving configuration compliance

OME achieves configuration compliance by comparing user created baselines to a device's configuration inventory. Configuration compliance baselines compare device configuration inventory attributes against the baselines' (the expected) attribute values. To create a baseline, a user selects a compliance template and devices. A device can have multiple baselines. Configuration inventory is obtained by creating and running an inventory job with the configuration option selected.

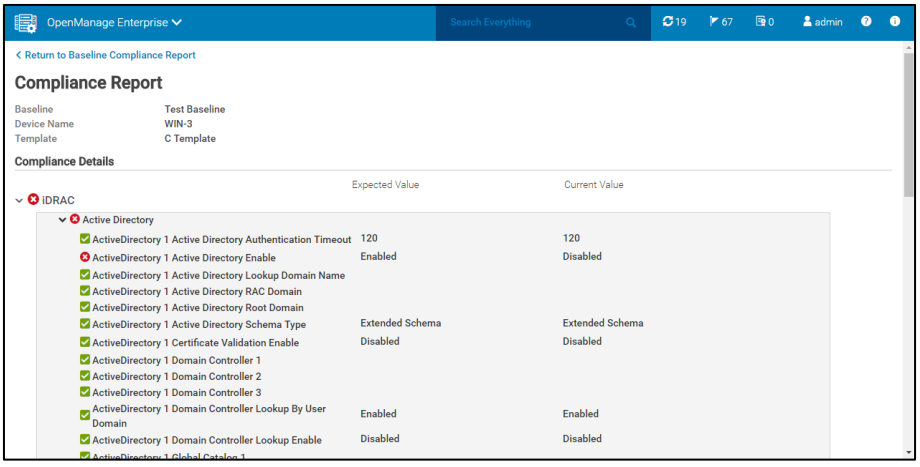

Figure 1: Example compliance report. Note the difference between the Expected Value and Current Value of the "ActiveDirectory 1 Active Directory Enable" attribute and how this status is rolled up to the group and component.

A compliance template can be created from a reference device or imported from a file. Compliance templates can be modified. You can change the values of a given attribute and choose to include or exclude the attribute from compliance evaluation.

Best Practices

- **Guideline 1: Create Compliance Templates from Configured Targets**
  Create a compliance template from a device that is already configured in an ideal way. If a device is already in a desired state, create a compliance template from the device to reduce the modifications needed for the compliance template.
- **Guideline 2: Only Include Necessary Configuration Options**
  Include only the configuration options you need for a compliance template. At the time of compliance template creation, check the configuration options (iDRAC, BIOS, NIC, etc.) that you want to check for compliance. This will make compliance operations faster.
- **Guideline 3: Modify the Compliance Template as Needed**
  Modify the compliance template as needed. Compliance templates are editable and many of the attributes have auto complete options and tool tip descriptions. Include or exclude individual attributes or entire sections.
- **Guideline 4: Adjust the Configuration Inventory Schedule**
  Create and schedule a configuration inventory task for off hours. The configuration inventory task can take anywhere from one to ten minutes to complete per device. Choose an appropriate interval (daily or on certain days of the week) for your environment.
- **Guideline 5: Make Baselines Component and Use Case Specific to your Policies**
  Make baselines specific to the policies of the datacenter and assign devices to multiple baselines as needed. An advantage of the baseline infrastructure is the ability to assign devices to multiple baselines. Utilize this by creating baselines specific to a section (iDRAC for example). This increases the likelihood that devices are compliant with the baseline and pinpoints the non-compliant component.
- **Guideline 6: Create Compliance Alert Policies**
  Setup alert policies for device compliance. An alert is generated when a configuration baseline compliance status changes. Create alert policies that send an email or perform an action when the compliance status changes.

Conclusions

The configuration baseline feature was developed for customers that need to know when and what configuration changed on a device. Configuration baseline compliance is ideal for environments that have similar models of hardware and have requirements on the configuration settings of the devices. This feature is available in the OpenManage Enterprise GUI and REST API.